Amendments to the Specification

Please replace the paragraph beginning on page 10, line 10 with the following rewritten paragraph:

With reference to Figure 2, the radio interface protocol architecture according to the 3GPP specifications will be described. The protocol entities described operate between:

- the user equipment UE ~~2~~ 6, and NodeB 26

and/or

- the user equipment UE ~~2~~ 6, and the RNC 24.

The division of protocol layers between NodeB 26 and RNC 24 is not described here further.

Please replace the paragraph on beginning on page 10, line 19 with the following rewritten paragraph:

The radio interface protocols can be divided into a control plane 50 and a user plane 52. The control plane 50 is used for all signaling between the UE ~~2~~ 6, and the RNC 24, and also between the user equipment UE ~~2~~ 6, and the core network CN 2. The user plane, ~~2~~ carries the actual user data. Some of the radio interface protocols operate only in one plane whilst some protocols operate in both planes.

Please replace the paragraph beginning on page 15, line 18 with the following rewritten paragraph.

The setting of the integrity key IK is as described herein. The key may be changed as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber is known. The key IK is stored in the visitor location register and transferred to the RNC, ~~10~~ when it is needed. The key IK is also stored in the mobile station until it is updated at the next authentication.

Please replace the paragraph beginning on page 20, line 11 with the following rewritten paragraph.

Since the identity of the signaling radio bearer is known by both the sender and the receiver, that is the user equipment UE 6 and the RNS 20, it is not necessary to send the identity information ~~explicitely~~ explicitly over the radio interface.

Please replace the paragraph beginning on page 21, line 12 with the following rewritten paragraph.

In a further embodiment of the present invention, the identity of the signaling radio bearer may be incorporated into the MESSAGE that is fed into the integrity algorithm. This is illustrated with number '3' in Figure 4. Since the identity of the signaling radio bearer is known by both the sender and the receiver, that is the mobile station and the RNS 20, it is not necessary to send the identity information over the radio interface with the actual MESSAGE. For example, if the MESSAGE has n bits ~~the~~ and the identity RB ~~IB~~ ID, has i bits, the actual 'MESSAGE' that would be fed into the integrity algorithm would have n+i bits. Thus, instead of just the MESSAGE alone being input to the integrity algorithm, the bit string fed into the integrity algorithm would become signaling radio bearer identity and the MESSAGE. This solution has no impact on the security issues (e.g. counter lengths) related to the integrity algorithm. This means that no parameter that is fed to the algorithm is made shorter: